Boston College International and Comparative Law Review

Volume 29 | Issue 2 Article 3

5-1-2006

Building Fortress India: Should a Federal Law Be Created to Address Privacy Concerns in the United States-Indian Business Process Outsourcing Relationship

Bryan Bertram

BUILDING FORTRESS INDIA: SHOULD A FEDERAL LAW BE CREATED TO ADDRESS PRIVACY CONCERNS IN THE UNITED STATES-INDIAN BUSINESS PROCESS OUTSOURCING RELATIONSHIP?

BRYAN BERTRAM*

Abstract: In the past few years, there has been a substantial surge in the use of Indian vendors by U.S. businesses for the performance of business processes. These types of engagements, referred to as business process outsourcing, routinely involve the transfer of sensitive personal data between U.S. and Indian firms. Thus, these types of transfers have raised concerns over the security of such data. The United States currently regulates these data transfers by industry sector. This policy contrasts sharply with other jurisdictions such as Canada, Japan, and the European Union where more broadly defined regulations set principles for the protection of data generally. This Note will examine whether the United States should enact broader based legislation in order to regulate the growing trend of business process outsourcing to India and protect sensitive data that gives rise to personal privacy concerns.

> *A line of neatly dressed workers files into the Golden Millennium, a shimmering glass-and-steel building in central Bangalore. One by one, they swipe ID cards through a reader, then empty their pockets and bags and stuff cell phones, PDAs, and even pens and notebooks into lockers as a dour security guard watches. Staffers ending their shifts, meanwhile, are busy shredding notes of conversations with customers. At the reception desk, visitors sign a daunting four-page form promising not to divulge anything they see inside—and even then are only allowed to peer into the workspace through thick windows.*[1]

* Bryan Bertram is an Executive Editor for the *Boston College International & Comparative Law Review.*

[1] Pete Engardio, *Fortress India?: Call Centers and Credit-Card Processors Are Tightening Security to Ease U.S. and European Fears of Identity Theft,* BUS. WK., Aug. 30, 2004, at 28, 28.

Introduction

The preceding example illustrates the importance Indian business places on the security of personal data when maintaining business process outsourcing (BPO) relationships.[2] This importance seems well-founded given the recent dramatic growth in the BPO sector of India's economy.[3] Many businesses already outsource or are considering outsourcing business functions that handle sensitive data.[4] As businesses continue to cut costs in order to improve their bottom line, they continue to outsource certain business processes that can be performed more cheaply in countries such as India.[5] In the context of these relationships, privacy of one's personal information has become an issue because of the highly sensitive nature of the data that often is transmitted in overseas BPO relationships.[6] As a consequence, the Indian government and Indian businesses have taken many steps towards improving the security of personal data passed in these relationships.[7]

Despite Indian measures, increasing scrutiny has come to bear on these relationships by the United States.[8] Numerous new legislative proposals have been introduced at both the state and federal levels.[9] This scrutiny and associated legislation can be frustrating to India, which believes it has made many good faith efforts at improving data security and perceives concerns in the United States to be largely unjustified.[10]

The purpose of this Note is to analyze the U.S.-Indian BPO relationship. This encompasses current U.S. law governing overseas BPO, its effects on the Indian government's data privacy regulation, as well as the reactions of U.S. and Indian firms. This Note argues that the United States and India should both enact laws of general applicability governing this relationship in order to correct current deficiencies as well as provide a clear set of standards with which U.S. and Indian businesses should comply and to which Indian law should conform.

---

[2] *See id.*

[3] *See* Paul Davies, What's This India Business? 43–45 (2004).

[4] *See id.*

[5] *See id.* at 21–22.

[6] *See, e.g.,* Rahul Sachitanand, *Lax Privacy Laws Hit Healthcare BPOs,* Econ. Times (Gurgaon, India), May 7, 2004, *available at* Factiva Doc. No. ECTIM00020040506e05700015 (explaining the sensitivity of patient files outsourced in healthcare BPO and concerns in the United States over security of this type of personal information).

[7] *See IT Industry Irked at TV Exposure,* Hindu (Chennai, India), Aug. 18, 2005, at 3.

[8] *See Safety Matters: Outsourcing to India,* Economist, Sept. 4, 2004, at 70, 70.

[9] *See id.*

[10] *See id.*

Part I of this Note will consider background and history of the United States-Indian BPO relationship by examining drivers behind the growth of the overseas BPO market and its effects on both nations. Part II of this Note will discuss the strengths and weaknesses of U.S. law in maintaining secure BPO transactions between U.S. and Indian firms. It will do so by assessing deficiencies in U.S. law as well as examining Indian efforts to conform to U.S. standards. This Note will conclude by summarizing the deficiencies that currently exist in the United States-Indian BPO relationship and proposing that the federal government adopt a law of general applicability to govern overseas BPO.

I. Background and History

Businesses are increasingly seeking to outsource processes that can be accomplished more cost-efficiently in overseas locations.[11] This type of outsourcing, known as business process outsourcing, is defined as a business engagement that transfers responsibility for ongoing management and execution of a business activity, process, or functional area to an external service provider in order to gain efficiencies and improve performance.[12] BPO arrangements are exceedingly complex because they entail the transfer and execution of one or more complete business processes or entire business functions to an external service provider.[13]

BPO now constitutes an enormous growth area for business and is the fastest growing segment of outsourcing arrangements.[14] Traditionally, BPO occurred domestically.[15] Nevertheless, advances in low-cost data transmission capability and cheap foreign labor pools have

---

[11] *See* Davies, *supra* note 3, at 21–22.

[12] Kapil Dev Singh, *Understanding the Business of Business Process Outsourcing, in* Business Process Outsourcing: Trends and Insights 56, 57 (ASSOCHAM) (2003). Background information on the conference where this publication was produced is available at http://www.assocham.org/bpo/bpo16072003.html (last visited Feb. 10, 2006).

[13] *See id.*

[14] *See* William A. Tanenbaum, *Information Technology and Business Process Outsourcing, in* PLI's Ninth Annual Institute for Intellectual Property Law, 220, 230 (PLI Pats., Copyrights, Trademarks, and Literary Prop. Course, Handbook Series No. G0-016V, 2003), *available at* WL 765 PLI/Pat 221. The term "outsourcing" was coined in 1988, but the phenomenon began as early as the 1950s and 1960s. William L. Deckelman, Jr., *Outsourcing: A Primer, in* PLI's 19th Annual Institute on Computer Law, 435, 439-40 (PLI Pats., Copyrights, Trademarks, and Literary Prop. Course, Handbook Series No. G0-004D, 1999), *available at* WL 547 PLI/Pat 435.

[15] *See* Fed. Deposit Ins. Corp., Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks 6 (2004), *available at* http://www.fdic.gov/regulations/examinations/offshore/offshore_outsourcing_06–04–04.pdf.

prompted a significant movement of BPO overseas.[16] The reasoning behind this shift is that foreign labor is cheaper than comparable domestic labor and quality levels typically do not decline in such a relationship.[17] Another desirable attribute of overseas BPO is the ability to realize around-the-clock operations—when the workday ends in the United States, it is just beginning in India.[18] Finally, businesses often turn to overseas BPO in order to focus efforts on "core" functions where the firm has a competitive advantage while allowing others to accomplish non-core functions.[19] The BPO movement is also self fueling; as some businesses choose to embrace overseas BPO in order to realize cost-efficiencies, other firms are forced to do the same in order to remain competitive.[20]

Two of the major areas of growth in overseas BPO have been the healthcare and financial services industries.[21] In healthcare, the use of offshore contractors has increased in recent years due to advances in information technology.[22] The movement towards electronic medical records and processing systems has allowed healthcare providers to shift certain functions off-site if they can be performed more cost-efficiently elsewhere.[23] This technology now allows services such as technical support, transcription, collation, billing, insurance claims' processing, and x-ray analysis to be sent overseas.[24] There are fifteen to twenty large and midsize vendors in India that service the healthcare market in both North America and Europe, employing about 5000 professionals.[25]

Financial services is another area in which overseas BPO relationships have often been created in order to realize business

---

[16] *Id.*

[17] Davies, *supra* note 3, at 29–30. In fact, the level of quality in BPO relationships with India may actually increase in comparison to domestic providers because work associated with BPO is often held in more high esteem in India than in the United States. *See id.* at 30.

[18] Fed. Deposit Ins. Corp., *supra* note 15, at 8.

[19] Davies, *supra* note 3, at 22–23. Focusing on a firm's core implies efficiency because it allows a firm to invest in its own competitive advantage while allowing third parties to accomplish other activities that the third party views as its own core. *Id.*

[20] Fed. Deposit Ins. Corp., *supra* note 15, at 8.

[21] *See* Tanenbaum, *supra* note 14, at 240.

[22] Kenneth N. Rashbaum, *Offshore Outsourcing of Health Data Services,* 16 Health Law. 24, 24 (2004).

[23] *See id.;* Davies, *supra* note 3, at 21–22.

[24] Rashbaum, *supra* note 22, at 24. For example, recent statistics show radiological outsourcing increasing by 7% per year with 12% of hospitals currently engaging in such a practice. Nathaniel H. Hwang, Comment, *The Concerns of Electronically Outsourcing Radiological Services Overseas,* 25 J. Legal Med. 469, 471 (2004).

[25] Sachitanand, *supra* note 6.

efficiencies.[26] For example, Deloitte Consulting, L.L.P. estimates that financial institutions utilizing overseas BPO relationships achieve an average cost savings of 39%.[27] It is estimated that 25,000 tax returns were completed by accountants in India in 2002 and that almost four times that amount were processed in 2003.[28]

India has been a major recipient of overseas BPO because it possesses an advantage that most other countries do not: a relatively well educated workforce.[29] Due to the increasing sophistication of the Indian workforce, India is no longer just a source for cheap code and call centers. BPO services offer opportunities for Western companies to access the skills of Indian accountants, scientists, lawyers, and other professionals.[30] Helping matters further is a favorable tax regime instituted by the Indian government that catalyzes BPO sector growth.[31] This confluence of advantages has helped the Indian tech sector, of which BPO is a part, to grow substantially in the past few years with revenues most recently surpassing the $3 billion mark.[32] McKinsey & Company recently predicted that revenues to Indian service companies would grow to $142 billion in 2008.[33] Further, U.S. businesses are heavily invested in India as a BPO location; General Electric (GE), for example, receives claims processing, credit evaluation, accounting, and other functions for eighty global GE branches from 12,000 employees in India.[34] The Indian BPO sector is one of the highest employment generators for young Indian graduates and has an annual growth rate of more than 100%.[35]

---

[26] *See* Tanenbaum, *supra* note 14, at 240.

[27] Fed. Deposit Ins. Corp., *supra* note 15, at 7. This report goes on to indicate that one in four institutions surveyed reported cost savings in excess of 50%. *Id.*

[28] Richard G. Brody et al., *Outsourcing Income Tax Returns to India: Legal, Ethical, and Professional Issues,* 74 CPA J. 12, 12 (Dec. 2004), *available at* 2004 WLNR 14649302.

[29] *See* Davies, *supra* note 3, at 30.

[30] *See* Andrew Baxter et al., *'Epidemic' Warning on Mobile Viruses,* Fin. Times (London), Feb. 23, 2005, at 2.

[31] Davies, *supra* note 3, at 46. In all reality, favorable tax policies are not directly aimed at the BPO sector. *See id.* Nevertheless, tax benefits aimed at the information technology (IT) sector of the Indian economy have been extended to encompass overseas BPO based on a theory referred to as IT enabled services (ITES). *Id.* Under the ITES tax scheme, if overseas BPO services are enabled by IT (virtually all are), they qualify as IT services and, therefore, also qualify for preferential tax treatment. *Id.*

[32] *See Tackling an Unseen Enemy,* Hindu (Chennai, India), Sept. 27, 2004, at 14.

[33] Davies, *supra* note 3, at 16.

[34] *E.g., id.*

[35] *IT Sector Highest Employer of Graduates*, Statesman (New Dehli, India), Dec. 20, 2005, *available at* LexisNexis Academic Doc. No. A20055121936-F7A4-GNW.

Overseas BPO transactions, of the kind between the United States and India, invariably implicate concerns over personal privacy.[36] According to a survey whose sample included 115 companies in India and the United States, 82% of the companies in the United States were concerned about information security practices in India.[37] Such concerns seem well justified because the two industries experiencing the most growth in outsourcing are financial services and health care, which are also two of the largest compilers of personal data.[38]

Privacy should be distinguished from confidentiality and trade secrets.[39] Privacy refers to the use and disclosure of personal information; it only applies to information specific to individuals.[40] Different jurisdictions have often defined privacy protection in different ways, but most definitions coalesce around a set of certain principles.[41] The fundamental principles underlying privacy protection are summarized in the Fair Information Practices defined by the Federal Trade Commission: (1) notice; (2) choice; (3) access; (4) security; and (5) enforcement.[42] Notice includes both notice that personal information is being collected as well as notice regarding any disclosure to a third party.[43] The "choice" principle refers to the notion that the consumer ought to retain the ability to opt out from use or disclosure of personal information by a third party.[44] Security involves protecting personal information from unauthorized access or misuse.[45] Access involves allowing an individual whose information has been collected the ability to contact

---

[36] *See* Francoise Gilbert, *Privacy Strategies in Outsourcing, in* The Outsourcing Revolution 2003: Protecting Critical Business Functions 523, 527 (PLI Pats., Copyrights, Trademarks, and Literary Prop. Course, Handbook Series No. G0-01E8, 2003), *available at* WL 767 PLI/Pat 523. Privacy can often be a loaded term, difficult to define and with many nuances. *See* Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation,* 54 Admin. L. Rev. 85, 88–94 (2002).

[37] Sudha Nagaraj, *BPO Fine But What About Data Privacy?*, Econ. Times (Gurgaon, India), Nov. 6, 2004, *available at* Factiva Doc. No. ECTIM00020041105e0b60004o.

[38] *See* R. Bradley McMahon, Note, *After Billions Spent to Comply with HIPAA and GLBA Privacy Provisions, Why Is Identity Theft the Most Prevalent Crime in America?*, 49 Vill. L. Rev. 625, 628 (2004).

[39] *See id.*

[40] Gilbert, *supra* note 36, at 528–29.

[41] *See id.* at 529.

[42] Hahn & Layne-Farrar, *supra* note 36, at 91–94. European Safe Harbor guidelines for United States businesses slightly expand upon the FTC definition listing onward transfer and data integrity as additional principles underlying data privacy protection. *Compare id. with* Davies, *supra* note 3, at 39.

[43] *See* Gilbert, *supra* note 36, at 530.

[44] *See* Hahn & Layne-Farrar, *supra* note 36, at 91.

[45] Gilbert, *supra* note 36, at 530.

the collecting entity with inquiries or complaints.[46] Security is rather self-evident from the name; reasonable steps should be taken to protect the security of personal information collected from individuals.[47] Finally, enforcement entails adequate remedies to cure violations when they do occur.[48]

In the most extreme example of a privacy breakdown, a Pakistani woman working remotely for a medical center in California threatened to post confidential patient records on the internet if she was not given a pay rise.[49] Pakistan is certainly not India, but in the perceptions of many, it was close enough.[50] For their part, Indian firms argue that their data security policies are world-class; ICICI OneSource, the outsourcing arm of India's largest private sector bank claims its policies are superior to any in Europe and the United States.[51] The lack of high profile incidents in BPO relationships supports this claim.[52] At ICICI OneSource, for example, there have only been two incidents of credit-card abuse, involving the theft of, respectively, $13 and $22.[53] Nevertheless, when contrasted with a recent FDIC study that lists India amongst countries with no data protection law, one must wonder whether the lack of incidents stems from India's measures or simply derives from a certain measure of luck.[54]

II. Discussion

A. *U.S. Regulatory Framework Governing Overseas BPO*

The United States has so far never adopted legal measures generally applicable to overseas BPO but rather relies upon narrow measures aimed at specific issues and industry sectors.[55] The approach is very different from other developed nations and organiza-

---

[46] *Id.*

[47] *See* Hahn & Layne-Farrar, *supra* note 36, at 93.

[48] *See id.* at 93–94.

[49] *See Safety Matters: Outsourcing to India, supra* note 8, at 70.

[50] *Id.*

[51] *Id.*

[52] *See id.*

[53] *Id.* Heartland Information Services, Inc., a Toledo, Ohio medical outsourcing company, reported in 2004 an extortion attempt by an Indian worker using personal data. Chris Seper, *Outsourcing Brings Identity-Theft Risk*, Plain Dealer (Cleveland, Ohio), May 24, 2004, at E4. This worker was subsequently arrested within twenty-four hours of the threat. *Id.*

[54] *See* Fed. Deposit Ins. Corp., *supra* note 15, at 20.

[55] *See* Hahn & Layne-Farrar, *supra* note 36, at 116.

tions such as Canada, Japan, and the European Union, which all have more generalized data privacy laws that incorporate more stringent requirements.[56] The typical justification for the approach taken in the United States is that enacting more generalized legislation could be prohibitively costly and lead to unintended consequences.[57] Nevertheless, it is interesting to note at the outset that the lack of any privacy legislation of general applicability has prompted the European Union to deem the United States as lacking adequate privacy protection.[58]

1. Identity Theft

At a very general level, the Identity Theft and Assumption Deterrence Act of 1998 makes identity theft a federal crime and provides an individual right of action for restitution as well as criminal sanctions.[59] The Act was passed in response to the patchwork of laws that previously addressed identity theft, and it carries strong penalties for violators.[60] The Act also cured deficiencies in enforcement of identity theft; the old patchwork of laws charged several different agencies with enforcement while the Act vests enforcement responsibility with the FTC.[61]

2. Health Information

Personal health information is protected by the Health Insurance Portability and Accountability Act of 1996, commonly referred to as HIPAA.[62] HIPAA was not originally written to protect privacy, rather, it was meant to facilitate health insurance transferability and the transfer of private information between entities.[63] HIPAA's privacy regulations

---

[56] *See* Kenneth A. Adler, *Recent Trends in Outsourcing: Understanding and Managing the Risks, in* 24TH ANNUAL INSTITUTE ON COMPUTER LAW, 389, 406 (PLI Pats., Copyrights, Trademarks, and Literary Prop. Course, Handbook Series No. G0-01K6, 2004), *available at* WL 781 PLI/Pat 389.

[57] *See* Hahn & Layne-Farrar, *supra* note 36, at 158–59.

[58] Gilbert, *supra* note 36, at 559. This label prompted a lengthy negotiation of safe harbor provisions for U.S. businesses in order to avoid costly impediments to the transfer of data between the United States and Europe. *Id.* A U.S. company that adheres to the safe harbor principles and completes the Department of Commerce's self-certification program will receive a presumption from all E.U. member states that its data privacy protections are adequate. *Id.*

[59] Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028 (2006)); s*ee* Hahn & Layne-Farrar, *supra* note 36, at 121.

[60] McMahon, *supra* note 38, at 629–31.

[61] *Id.*

[62] Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 29 U.S.C. and 42 U.S.C. (2006)); s*ee* McMahon, *supra* note 38, at 645.

[63] McMahon, *supra* note 38, at 644.

were enacted by the Department of Health and Human Services subsequent to the legislation itself.[64] HIPAA regulates the outsourcing of data through the Privacy Rule which was published in December, 2000.[65] The Privacy Rule regulates access through an opt-in choice mechanism to provide privacy for patient information.[66] This opt-in mechanism only allows disclosure of personal information if the patient expressly authorizes such disclosure.[67]

Despite restrictions on access, this rule has several enforcement problems because it has difficulty reaching offshore BPO providers in countries such as India.[68] HIPAA does not directly address the possibility of privacy breakdowns by contractors.[69] The Privacy Rule does recognize that medical providers will inevitably outsource some of their functions and designates the contractors for such work as Business Associates (BAs).[70] BAs are subject to the same regulations as the initial provider because the Privacy Rule requires BAs to enter into contractual arrangements that conform with the provisions of the Privacy Rule.[71] Problems arise because most medical providers initially outsource to domestic firms that, in turn, will outsource to offshore firms such as those in India.[72] Even though those Indian BAs are subject to the same provisions of the Privacy Rule as everyone else, those BAs are so attenuated from the original provider that promises may be hollow at best.[73] Exacerbating this difficulty is a lack of offshore jurisdiction granted to the Department of Health and Human Services (HHS) which is charged with enforcing the Privacy Rule.[74] Moreover, even though BAs must contract with the provider, the provider has no obligation to monitor the conduct of any of its BAs.[75]

---

[64] *See id.* at 645. The Privacy Rule is codified at 45 C.F.R. § 160.103 (2006).

[65] *See* Gilbert, *supra* note 36, at 539.

[66] McMahon, *supra* note 38, at 648.

[67] *Id.*

[68] *See* Rashbaum, *supra* note 22, at 25.

[69] *See id.*

[70] *Id.*

[71] *See id.*

[72] *See id.*

[73] *See* Rashbaum, *supra* note 22, at 25.

[74] *See id.*

[75] *Id.* Even if a medical provider does monitor the activities of its business associates, the great distances involved can often serve to mask privacy problems. Jaikumar Vijayan, *Security Expectations, Response Rise in India: Increasingly Tough Demands from U.S. Clients Spark Change,* COMPUTERWORLD, Aug. 30, 2004, at 6. For example, a growing BPO firm that was in the process of relocating to a larger facility decided to move some of its servers to an internet café during a period of delay over the new facility's opening. *Id.*

Finally, HHS is the only entity that may enforce the Privacy Rule.[76] The Rule provides no private right of action for health care consumers.[77] This deficiency has not gone unnoticed and Senator Hillary Rodham Clinton of New York has introduced a bill which would require create a private right of action for any misuse of this information by an offshore concern.[78] Some help is also provided by more stringent state laws that are not preempted by HIPAA, but not every state has such laws.[79]

3. Financial Information

Federal regulation of financial services overseas BPO is accomplished through a web of federal statutes.[80] For example, the Consumer Credit Reporting Reform Act of 1996 places restrictions on credit card agencies in using personal data, one notable restriction being disclosure only in instances of business need.[81] At the center of federal financial regulation is the Financial Services Modernization Act of 1999, commonly referred to as the Gramm-Leach-Bliley Act (GLBA), which provides privacy protection for personal data.[82] One of the strengths of this Act is its scope, covering financial advice, credit counseling, credit cards, data processing, investments, lending check cashing, wire transfers, tax preparation, debt collection, or providing credit, insurance, lay-a-way, financing, brokerage, financial aid, lease, or account services.[83] The GLBA requires financial institutions to make full disclosure of their privacy policies to consumers.[84] The GLBA further requires that entities subject to the Act implement substantial security measures and demands that the agencies that implement the GLBA

---

[76] *See* Rashbaum, *supra* note 22, at 25–26

[77] *See id.*

[78] Safeguarding Americans From Exporting Identification Data Act (SAFE-ID Act), S. 810, 109th Cong. (2005); Rashbaum, *supra* note 22, at 27.

[79] *See* Rashbaum, *supra* note 22, at 26.

[80] *See id.* at 28 (discussing financial data).

[81] Pub. L. No. 104-208, §§ 2403, 2413, 110 Stat. 3009, 3009-430, 3009-447 (1996) (codified at 15 U.S.C. §§ 1681b(a), 1681s-2 (2006)); Hahn & Layne-Farrar, *supra* note 36, at 122.

[82] Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified at 15 U.S.C. §§ 6801–6809 (2006)); *see* Hahn & Layne-Farrar, *supra* note 36, at 123.

[83] *See* Gilbert, *supra* note 36, at 535. The GLBA derives its sweeping scope from its applicability to the term "financial institutions" which was not defined in the Act but has subsequently been defined broadly by the FTC. McMahon, *supra* note 38, at 634–35.

[84] James X. Dempsey & Lara M. Flint, *Commercial Data and National Security,* 72 Geo. Wash. L. Rev. 1459, 1479 (2004).

publish extensive security standards.[85] The GLBA requires that any outsourcing concerns, even if offshore, must be under contractual agreement to comply with all applicable standards.[86] The Federal Banking Agencies have extended the responsibilities of financial institutions to also monitor the activities of any third party to which it transfers sensitive data.[87] Further, the FTC has indicated its willingness to prosecute any abuses of personal financial data under the GLBA.[88]

Unfortunately, the GLBA has many deficiencies.[89] Its opt-out mechanism for limiting access to sensitive data is a point of controversy for GLBA's critics.[90] Some have argued that few consumers actually exercise this option because consumers would have to struggle through fine print to learn how to protect their privacy.[91] More narrowly, consumers do not have the normal opportunity to opt out of a transfer of their information overseas when the purpose of the transfer is to "service or process a financial product that the customer requested or authorized . . . or maintain or service the customer's account."[92] This is significant when it is considered in relation to a recent FDIC report indicating that 15% of the financial services cost current cost base ($356 billion) is expected to move offshore in the next five years.[93]

4. State Regulation

Despite the presence of these federal statutes regulating aspects of overseas BPO, there remain a myriad of state statutes and common law also affecting BPO transactions.[94] Many states first addressed these

---

[85] Gilbert, *supra* note 36, at 536.

[86] *See id.*

[87] Fed. Deposit Ins. Corp., *supra* note 15, at 14.

[88] *See* Rashbaum, *supra* note 22, at 28. In a letter to Congressman Edward Markey, FTC Chairman Timothy Muris wrote, "[s]imply because a company chooses to outsource some of its data processing to a domestic or offshore provider does not allow that company to escape liability for any failure to safeguard the information adequately." *Id.* Despite the reassuring tone of its rhetoric, the FTC has not yet brought any actions against an overseas provider for any breach of confidential information. *Id.*

[89] *See id.* The GLBA has many critics who argue that its protections have not provided any real privacy enhancements. Hahn & Layne-Farrar, *supra* note 36, at 130. For example, according to former Federal Trade Commission chairman Timothy J. Muris, "Acres of trees died to produce a blizzard of barely comprehensible privacy notices." *Id.*

[90] *See* McMahon, *supra* note 38, at 635–36.

[91] *See id.* at 636.

[92] *See* Rashbaum, *supra* note 22, at 28 (citing § 502(c) of the Gramm-Leach-Bliley Act, 15 U.S.C. § 802(e) (2006)).

[93] *See* Fed. Deposit Ins. Corp., *supra* note 15, at 2. The numbers in the FDIC study were compiled by Deloitte Consulting, LLP. *Id.*

[94] Gilbert, *supra* note 36, at 534.

types of privacy issues under a theory of tort, and many still rely on the common law that developed from such an approach.[95] Beyond the common law, state legislatures have passed numerous statutes addressing very narrow privacy concerns.[96] Some states have even experimented with broader measures to guard personal privacy.[97] For example, California recently enacted legislation to compel notification of individuals when their information has been improperly appropriated by a third party, a requirement that cuts across industry lines.[98]

In addition to a complex regulatory framework, it is increasingly obvious that many federal and state efforts to patch privacy holes are not so much aimed at securing privacy as they are at preventing the outsourcing of domestic jobs.[99] An example of such veiled legislation lies in a recent bill proposed by Senator George Voinovich of Ohio that would restrict the outsourcing of work conducted by any companies with government contracts, a measure that is in no way tied to privacy concerns.[100] An amendment to this bill proposed by Senator Christopher Dodd would take the provisions one step further to include state contracts funded with federal money.[101] This type of legislation is not limited the federal level; for example, Virginia currently has four anti-BPO bills pending, and the Secretary of Technology for Virginia acknowledges that job preservation is a key motivator.[102]

3. Self-Regulation

Given the lack of a clear regulatory framework or any privacy law of general applicability, the federal government has also often encouraged self-regulation.[103] Self-regulation can involve such measures as companies passing their own data privacy policies.[104] Several or-

---

[95] *See id.*

[96] *Id.*

[97] *See, e.g.,* Timothy H. Skinner, *California's Database Breach Notification Security Act: The First State Breach Notification Law is Not Yet a Suitable Template for National Identity Theft Legislation,* 10 Rich. J.L. & Tech. 1, 21–23 (2003).

[98] *See generally id.*

[99] *See Safety Matters: Outsourcing to India, supra* note 8, at 70.

[100] *See Anti-BPO Steps: What to Worry About,* Econ. Times (Gurgaon, India), June 18, 2004, *available at* Factiva Doc. No. ECTIM000200406l8e06i000bx.

[101] *See id.*

[102] *Id.*

[103] *See* Gilbert, *supra* note 36, at 561.

[104] *Id.* An example of such a company policy is that of Amazon which reads:

> We employ other companies and individuals to perform functions on our behalf . . . . They have access to personal information needed to perform their functions,

ganizations now provide seals of approval for these types of privacy policies if they meet certain minimum requirements.[105] Further, Indian businesses have enormous incentive to avoid privacy scandals so as to avoid the bad publicity associated with a privacy breakdown.[106] The Bush Administration favors self-regulation to secure privacy.[107]

B. *The Indian Reaction to U.S. Data Privacy Law*

Currently, the only law that *specifically* governs Indian businesses' protection of personal data derives from foreign jurisdictions such as U.S. or European Union data privacy laws.[108] Nevertheless, Indian lawmakers have enacted Indian laws that indirectly regulate Internet commerce.

Indian businesses have typically been very concerned about privacy concerns and overseas BPO transactions.[109] This should not be surprising given the large contributions of the BPO sector to India's economy.[110] In order to quell both U.S. political and business concern, India has enacted several measures to prevent any data privacy abuse.[111]

1. Information Technology Act of 2000

Most prominent was India's adoption of the Information Technology Act of 2000.[112] This Act was based on the Model Law on Electronic Commerce adopted by the United Nations (U.N.) in 1997.[113] At a broad level, this legislation was an important step forward be-

---

> but may not use it for other purposes. . . . Other than as set out above, you will receive notice when information about you might go to third parties, and you will have an opportunity to choose not to share the information.

Id. Company policies often have real enforcement teeth because failure to comply with one's own privacy policy may open a company up to prosecution based upon misrepresentation or unfair and deceptive practices. *Id.* at 563.

[105] *Id.* at 562.

[106] *See* Stella M. Hopkins, *Outsourcers Are Anxious to Safeguard Your Privacy,* CHARLOTTE OBSERVER, Feb. 12, 2005, at 1D.

[107] Skinner, *supra* note 97, at 60.

[108] *See id.*

[109] *See* Engardio, *supra* note 1, at 28.

[110] *See* DAVIES, *supra* note 3, at 16.

[111] *See* Pavan Duggal, *Legal Issues Confronting the Indian Outsourcing Industry, in* BUSINESS PROCESS OUTSOURCING: TRENDS AND INSIGHTS, *supra* note 12, at 62, 62.

[112] *See id.* at 62.

[113] Theodore P. Augustinos et al., *International Banking and Finance,* 35 INT'L LAW. 287, 319 (2001).

cause it placed India amongst only a few countries that currently regulate Internet transactions.[114] The opening provisions of the Act read:

> An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage . . . .[115]

Although the Act is not generally applicable to data privacy specifically, it does define a certain universe of "electronic" activity for regulation, and the typical BPO relationship is a subset of this universe.[116] Of specific interest to BPO transactions with the United States are Sections 4, 5, 7, and 79 of the Act.[117] The aforementioned sections are applicable to overseas BPO because they define data, mandate standards for the authentication and retention of that data, and provide penalties for violations of these provisions.[118] Nevertheless, even though the Act defines data, it is completely silent on the issues of data protection.[119]

One of the most important aspects of this Act is the creation of a special appellate court for violations of the Act's provisions.[120] Indian courts are notorious for being exceedingly slow in their resolution of disputes.[121] As one scholar has noted, "[The Indian legal system] has all the flexibility and user-friendliness of a land mine, threatening to blow up should you or anyone close to it look like moving."[122] Thus, the creation of an independent appellate branch specifically tasked with overseeing computerized transactions signals a dedication on the part of the Indian government to ensuring that these transactions are dealt with expeditiously.[123] It is important to note, however, that even crea-

---

[114] *See* i*d.*

[115] Information Technology Act 2000, No. 21 of 2000 (India), *available at* http://www.mit.gov.in/itbill2000.pdf.

[116] *See* Duggal, *supra* note 111, at 62.

[117] *See id.* at 62–67.

[118] *See id.*

[119] *Id.* at 67.

[120] *See* Stephanie Overby, *India to Adopt Data Privacy Rules,* CIO Mag., Sept. 1, 2003, at 28.

[121] *See* Dilip Mookherjee, *Legal Institutions and Economic Performance, in* The Crisis in Government Accountability: Essays on Governance Reforms and India's Economic Performance 123 (2004). For example, simple matters such as dissolution of a partnership, where both partners have previously agreed to terms, have been known to languish in the Indian court system for as long as ten years. Davies, *supra* note 3, at 159.

[122] Davies, *supra* note 3, at 159.

[123] *See* Overby, *supra* note 120, at 28.

tion of a special judiciary unit may not completely relieve the problem of court delays.[124] Delays in Indian courts are a function of two problems: "an insufficiently slow growth in the number of sanctioned positions, and a growth in the number of unfilled vacancies."[125] While creating a special judiciary unit might cure the former problem, it does nothing to address the latter because it provides no guarantee that the newly created judicial positions will be properly funded and staffed.[126]

2. Proposed New Privacy Legislation

Despite the progress made with the Information Technology Act of 2000, India still lacks specific law regarding the protection of personal data in overseas BPO transactions.[127] India's government is currently working on new legislation to quell growing privacy concerns.[128] The government plans to study laws both in the European Union and the United States to ascertain how to best structure India's own laws.[129] Any proposal ultimately adopted by the Indian parliament will likely reflect the European Union's requirements on data privacy which served as India's original impetus to review its own laws.[130] Nevertheless, U.S. business concerns will likely play a role too by inducing India to refrain from setting standards that are too stringent and costly.[131]

3. Self-Regulation

Some of India's efforts at complying with the demands of U.S. privacy law have originated in the private sector rather than the legal sector.[132] The National Association of Service & Software Companies (NASSCOM) is India's national information technology trade group and has been the driving force behind many private sector efforts to improve data security.[133] According to Sunil Mehta, Vice President of NASSCOM, "We want to make India kind of a Fort Knox of informa-

---

[124] *See* Mookherjee, *supra* note 121, at 124–29 (describing the causes of mounting court delays in India).

[125] *Id.* at 125.

[126] *See id.*

[127] *See* Duggal, *supra* note 111, at 67.

[128] *IT Industry Irked at TV Expose, supra* note 7, at 3.

[129] Sachitanand, *supra* note 6.

[130] *See* Overby, *supra* note 120, at 28.

[131] *See* Bureau of Indus. & Sec., U.S. Dep't of Commerce, HTCG Dialogue on Defense Technology, Data Privacy, and Export Licensing (2004), http://www.bis.doc.gov/InternationalPrograms/HTCG_Dialogue.htm.

[132] *See Safety Matters: Outsourcing to India, supra* note 8, at 70.

[133] *See id.*

tion of the world."[134] NASSCOM has been one of the contributors to efforts to tighten the Information Technology Act 2000.[135] NASSCOM also plans to have the security practices of all its members audited by international accounting firms.[136] Additionally, NASSCOM directly contributes to the development of legal enforcement mechanisms.[137] For example, in Mumbai (Bombay), a center of Indian commerce, NASSCOM has taught a dozen police officers the basics in fighting cyber-crime.[138]

Because Indian firms have gone to such lengths to protect data security, a new market, which is ancillary to the BPO market, has emerged.[139] Long Island-based Verint Systems Inc. provides systems used for video and voice surveillance at a cost of $1000 per worker.[140] Indian firms also pay up to $300 per worker for background checks that can take several weeks to compile.[141] Cyrca Data Security Solutions, a Toronto-based IT security, privacy and, compliance company, has also entered the Indian market to provide consultancy services regarding outsourcing.[142]

Given the extensive measures that Indian business and government have undertaken in order to meet privacy concerns, it seems neither unnatural nor unfair that they expect a positive perception of Indian data security.[143] Yet, most of this demand for respect has gone unrequited in the United States as political figures continue to use privacy as a smokescreen for efforts to curb outsourcing and protect American jobs.[144] Thus, one of the biggest problems in the U.S.-Indian relationship does not implicate legal or private sector issues but, rather, perception by India that efforts to meet U.S. demands will be dealt with fairly.[145] U.S. policymakers who advocate restrictions in overseas BPO to

---

[134] Hopkins, *supra* note 106, at 1D.

[135] *Outsourcing to India: Safety Matters, supra* note 8, at 70.

[136] *See id.*

[137] *See* Edward Luce, *India Acts to Protect Call Centre Security: Outsourcing Companies Know Even a Single Leak of Sensitive Information Could Destroy Them,* Fin. Times (London), Oct. 14, 2004, at 11; Hopkins, *supra* note 106, at 1D. Similar forces are planned for eight other Indian cities. *Id.*

[138] *Id.*

[139] *See, e.g., Cyrca Data to Enter Indian Market,* Econ. Times (Gurgaon, India), Dec. 16 2004, *available at* Factiva Doc. No. ECTIM000200412l5e0cg00013.

[140] Engardio, *supra* note 1, at 28. Verint has already signed up over 100 call centers in India for use of its services. *Id.*

[141] *Id.*

[142] *Cyrca Data to Enter Indian Market, supra* note 139.

[143] *See Safety Matters: Outsourcing to India, supra* note 8, at 70.

[144] *See id.*; *Anti-BPO Steps: What to Worry About, supra* note 100.

[145] *See Safety Matters: Outsourcing to India, supra* note 8, at 70.

India often cite both privacy and employment concerns as their motivations.[146] This only serves to hurt efforts at improved data privacy because India views these concerns more as an excuse to stem job loss than any real concern over privacy.[147] Further, this perception spans both continents: U.S.-Indian citizens share India's concerns over anti-BPO trends.[148] Anti-BPO efforts by U.S. policy makers have strained the U.S.-Indian relationship by creating an Indian perception that privacy concerns have become the hot new excuses for an age-old movement to erect barriers to trade and stem the outsourcing of U.S. jobs.[149]

III. Analysis

The preceding discussion illustrates the narrow, industry approach of U.S. law to overseas BPO.[150] At the most general level, no federal law defines a universal standard for personal privacy.[151] Although generalized privacy restrictions exist for information policy within the federal government, Congress has basically defaulted to a market-oriented model that is supplemented by more narrowly defined pieces of legislation.[152] Use of self-regulation by business entities then supplements these protections.[153] This contrasts sharply with the more systematic and wide reaching forms of legislation employed by member nations of the European Union, as well as Canada and Japan.[154]

1. Benefits and Detriments of Sectoral Regulation

The traditional justification for this sectoral approach to privacy legislation is utilitarian in nature, arguing that broader protections are not cost-benefit justified.[155] This type of utilitarian balancing usually

---

[146] *See* Engardio, *supra* note 1, at 28 (discussing Indian resentment over anti-BPO legislation in the United States, even though India has made large investments in data security and has had few breakdowns).

[147] *See id.*

[148] *See generally* Ishani Duttagupta, *Outsourcing Row Tilts Indians Towards Bush,* Econ. Times (Gurgaon, India), Oct. 29, 2004, *available at* Factiva Doc. No. ECTIM00020041027 e0as00007.

[149] *See* Engardio, *supra* note 1, at 28.

[150] *See* Hahn & Layne-Farrar, *supra* note 36, at 116.

[151] *See id.*

[152] *See id.*; James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy,* 76 U. Colo. L. Rev. 1, 1–2 (2005).

[153] *See* Nehf, *supra* note 152, at 1–2.

[154] *See* Adler, *supra* note 56, at 406.

[155] *See* Nehf, *supra* note 152, at 2–3.

favors less restrictive regulation that is narrower in scope.[156] Given this methodology, the current patchwork of sectoral laws is not all that surprising.[157]

The utilitarian approach to privacy balancing is open to criticism.[158] Cost-benefit analysis often favors the party that can better quantify the values for its position which, in the context of the privacy debate, is business seeking less regulation and less cost.[159] Further, some privacy advocates believe that the debate should not be utilitarian at all' rather, they believe that people have certain rights to privacy that should be protected without reference to cost.[160]

The narrowness of U.S. federal privacy policy is particularly evident when contrasted with the policies of the European Union.[161] Countries enjoying membership in the European Union have enacted laws regulating personal data.[162] While each law may contain somewhat different content, the European Union has harmonized these laws into a general framework by requiring individual countries to follow guidelines set forth in the European Union Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data.[163] These guidelines include requirements similar to the previously discussed principles of notice, security, access, and enforcement.[164] The European Union directive creates a guideline set of protections that every country must meet.[165] Countries are, however, free to institute more stringent requirements as they see fit.[166]

Most notably, the European Union directive creates an omnibus right of action, whereby data subjects can sue a data collector for misuse of data and receive monetary damages with fines as high as $500,000 in some countries.[167] "Individuals must be able to enforce their rights rapidly . . . and without prohibitive cost."[168] Finally, there must be an institutional mechanism allowing for investigation of com-

---

[156] *See id.*
[157] *See id.* at 2.
[158] *See id.* at 29–30.
[159] *See id.* at 29.
[160] *See* Nehf, *supra* note 152, at 3.
[161] *See* DAVIES, *supra* note 3, at 38; Adler, *supra* note 56, at 406.
[162] Gilbert, *supra* note 36, at 533.
[163] *Id.*
[164] *See id.*; *supra* notes 42–48 and accompanying text.
[165] *See* Gilbert, *supra* note 36, at 557.
[166] *See id.*
[167] *See id.* at 533–34.
[168] *Id.* at 558.

plaints.[169] Mandating such a set of legal enforcement mechanisms ensures that EU law never encounters a deficiency such as that associated with HIPAA: lack of a private right of action over a data privacy violation.[170]

Nevertheless, generalized legislation such as the European Union directive is not without its criticisms.[171] First, generalized statutory language always runs the risk of becoming out of date in quickly shifting technological environments.[172] Further, legislation proper for one sector of business may be over- or under-restrictive for another.[173] Generalized laws lose the ability of sectoral legislation in their ability to target specific protections to specific industries.[174] Finally, generalized legislation creates certain costs to doing business that could potentially place a country at a disadvantage in the marketplace.[175]

2. Need for Default Rules

Despite these shortcomings, it would still appear advisable that the United States adopt some of the philosophies of its European neighbors and implement some form of general applicability law to overseas BPO in order to govern the U.S.-Indian BPO relationship.[176] Establishing a set of principles governing overseas BPO would be beneficial because it would set a minimum set of standards for data privacy to which all BPO relationships would have to conform.[177] Model principles of this sort are readily available in the form of the European model as well as the previously discussed Fair Information Practices promulgated by the Federal Trade Commission.[178] Finally, it would help to eliminate

---

[169] *Id.*

[170] *Compare* Gilbert, *supra* note 36, at 557 (explaining the European system whereby the E.U. Directive creates an omnibus enforcement mechanism), *with* Rashbaum, *supra* note 22, at 25 (explaining enforcement deficiencies in HIPAA, including lack of a private right of action and difficulties in reaching offshore contractors).

[171] *See* Hahn & Layne-Farrar, *supra* note 36, at 118–20.

[172] *See id.*

[173] *See id.*

[174] *See, e.g., id.* (explaining how "the move in outsourcing . . . becomes exceedingly difficult under the Directive's restrictions on transborder transmissions" because it is overrestrictive in relation to current business needs).

[175] *See id.*

[176] *See* Gilbert, *supra* note 36, at 559 (explaining that other countries have adopted privacy laws similar to the directive adopted by the European Union).

[177] *See id.* (explaining the minimum principles of data privacy set forth in the E.U. Directive).

[178] *See id.* at 557–58 (listing the principles of data privacy set forth in the E.U. Directive); Hahn & Layne-Farrar, *supra* note 36, at 91–94 (listing the principles of data privacy set forth by the FTC).

differing protections and deficiencies across sectors.[179] For example, HIPAA has an enforcement deficiency because it does not provide a private right of action, whereas GLBA, while it does not have a similar enforcement deficiency, has a choice deficiency because it does not include an opt-out provision for overseas BPO.[180]

One of the considerations in drafting such generalized legislation should be a utilitarian cost-benefit balancing to create default rules protective enough to guard data privacy.[181] This calculus should not, however, be so restrictive that it kills the proverbial goose that lays the golden eggs by exacting such high costs that overseas BPO loses most of its business efficiencies.[182] For example, compliance with HIPAA in its first year cost an estimated $3 billion. Crafting equally restrictive provisions across the entire spectrum of overseas BPO would, by extension, potentially be prohibitively costly.[183] Such analysis is important because broad-based privacy legislation has often been criticized on the grounds that it would not be cost justified.[184] Nevertheless, although it is broader than a sectoral approach to regulating overseas BPO, a law of general applicability would still be narrow because it would only apply with a specific type of outsourcing transaction, BPO, and it would only apply to that transaction when it occurs in an overseas relationship.[185] Thus, cost-benefit analysis is not completely incompatible with a law of general applicability for overseas BPO.[186]

Of particular importance would be enforcement provisions.[187] Creating a general right of action for data privacy violations would

---

[179] See *infra* note 180 and accompanying text.

[180] *See* McMahon, *supra* note 38, at 637 (explaining that consumers do not have the normal opt-out choice associated with the GLBA under instances where information is shared to perform services for the financial institution); Rashbaum, *supra* note 22, at 25 (explaining enforcement deficiencies within HIPAA).

[181] See *infra* note 182 and accompanying text.

[182] *See* Hahn & Layne-Farrar, *supra* note 36, at 158–59 (explaining the dangers of broadly worded privacy legislation because of the possibility that such legislation could create prohibitive costs).

[183] *See* McMahon, *supra* note 38, at 650.

[184] *See* Hahn & Layne-Farrar, *supra* note 36, at 158–59.

[185] *Cf.* Hahn & Layne-Farrar, *supra* note 36, at 159 (explaining that privacy legislation of more narrow concern, focused on particular issues, would be more likely to be cost-benefit justified).

[186] *See id.*

[187] *See, e.g.*, Rashbaum, *supra* note 22, at 25 (pointing out the lack of a private right of action in HIPAA which severely weakens enforcement in the healthcare sector).

cure already existing deficiencies in that regard.[188] Further, given the difficulty in finding timely redress in Indian courts, such a provision would assure that those finding their rights violated would always have some form of expeditious recourse.[189]

Also worth careful scrutiny are principles detailing notice and choice.[190] Notice is important because it increases consumer knowledge as to what their privacy rights are.[191] At the same time, too much knowledge could be a bad thing in the context of privacy.[192] Just to comply with the GLBA, around 40,000 financial institutions were compelled to mail 2.5 billion privacy notices between the Act's implementation and June, 2001.[193]

Choice should be limited on a careful basis.[194] Default rules allowing for opt-out choice mechanisms should be mandated to guarantee privacy because a general rule of opt-in choice would be far too costly to BPO relationships.[195] Such a general rule would not necessarily preclude specific government action to protect particularly sensitive data or sectors with opt-in mechanisms; it would only preclude their costly widespread use.[196]

Some form of overseas BPO legislation would also signal to India that U.S. regulation still focuses on privacy issues rather than employment concerns.[197] With a slew of legislative proposals aimed at restricting overseas BPO, India has, justifiably, become extremely suspicious that U.S. efforts are not really aimed at privacy but, rather, at jobs.[198] These suspicions were only bolstered by much of the anti-outsourcing of jobs rhetoric during the 2004 presidential election.[199] Passing legislation targeted specifically at the principles of privacy protection in overseas BPO would help to refocus efforts away from job loss and back on

---

[188] *See* Gilbert, *supra* note 36, at 557–58 (detailing the numerous enforcement provisions present in the E.U. directive); Rashbaum, *supra* note 22, at 25 (explaining the lack of any individual right of action for HIPAA violations in medical overseas BPO).

[189] *See* MOOKHERJEE, *supra* note 121, at 125.

[190] *See* Hahn & Layne-Farrar, *supra* note 36, at 91–92, 159–60.

[191] *See id.*

[192] *See id.* at 130.

[193] *See id.*

[194] *See id.* at 159–60.

[195] *See id.*

[196] *See* Hahn & Layne-Farrar, *supra* note 36, at 159–60.

[197] *See* Engardio, *supra* note 1, at 28 (discussing Indian concerns that U.S. privacy legislation is not really aimed at privacy concerns but, rather, at stopping the outflow of U.S. jobs); *Anti-BPO Steps: What to Worry About, supra* note 100.

[198] *See* Engardio, *supra* note 1, at 28.

[199] *See* Duttagupta, *supra* note 148.

privacy.[200] In turn, such a refocusing could potentially help improve India's confidence in the sincerity of U.S. motives.[201]

Finally, beyond a utilitarian perspective, generalized legislation regarding overseas BPO would help to protect data privacy based on the notion that individuals have a right to such protection.[202] It is easy to collapse the debate surrounding overseas BPO regulation into a tidy economic cost-benefit box because the costs of compliance are easy to quantify.[203] Further, it is often difficult to quantify the benefits of privacy protections because they are not amenable to numerical valuation.[204] Nevertheless, the ease of calculating cost with the difficulty of calculating benefit can lead to under-protection if a utilitarian philosophy dominates.[205] Moreover, a utilitarian approach may not be reconcilable with certain U.S. legislation either.[206] For example, the preamble to HIPAA expressly recognizes that medical privacy is a "fundamental right" different from "ordinary economic good[s]."[207]

The central problem with restricting discussion of overseas BPO regulation to only utilitarian concerns is that such restriction serves to commodify privacy.[208] Yet, most would probably agree that personal privacy is more than a mere economic good.[209] Loss of privacy is seen as a loss of personal autonomy, an affront to human dignity, or even an intrusion into one's core-self.[210] This theory would support a generalized law of overseas BPO to govern relationships such as the U.S.-Indian BPO relationship because privacy constitutes more than a mere economic commodity that is not easily valued by utilitarian cost-benefit balancing and demands such protections despite high costs.[211]

---

[200] *See* Engardio, *supra* note 1, at 28.

[201] *See* Engardio, *supra* note 1, at 28.

[202] *See generally* Nehf, *supra* note 152.

[203] *See id.* at 29.

[204] *See id.* at 55.

[205] *See id.* at 2–3.

[206] *See id.* at 53.

[207] *See id.* (quoting Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,464 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160, 164)).

[208] *See* Nehf, *supra* note 152, at 30.

[209] *See id.*

[210] *See id.*

[211] *See id.*

Conclusion

In order to improve the security of personal privacy in the U.S.-Indian BPO relationship, the United States ought to consider adoption of a general law of applicability, defining data privacy standards for these types of relationships. Although there have not yet been any high-profile instances of privacy breakdowns in the context of the U.S.-Indian relationship, deficiencies currently exist in protections that should be addressed.

In the two primary sectors where overseas BPO relationships occur, financial services and medical services, deficiencies exist that could compromise personal privacy. In the financial services sector, primarily governed by the GLBA, these include the lack of opt-out mechanisms for overseas BPO. In the medical services sector, lack of an individual private right of action undermines the principle of enforcement and furthers the possibility of privacy breakdowns. Although not a complete list, the deficiencies in these two sectors highlight the primary structural problem in U.S. regulation. These inadequacies span the major sectors where overseas BPO occurs, and they vary by sector. Therefore, the only means of correcting them under the current approach would be the inefficient and time-consuming process of crafting narrow legislation to deal with each sector's own problems.

U.S. policymakers ought to consider creating a law of general applicability governing oversees BPO transactions in order to rectify many of these shortcomings and provide a more consistent data privacy protection policy. Such a law would provide a set of governing principles applicable to *all* sectors of overseas BPO and set a floor of protections for data privacy.

Of particular importance for such a policy would be the principles of enforcement, notice, and choice. Creation of a general right of action for those harmed by privacy violations would cure any such deficiencies in sectoral legislation. Emphasizing consumer notice provisions would be a cost-efficient manner to promote better data privacy protections. Finally, creating a default opt-out choice mechanism would ensure that all consumers have the option to refrain from having their personal information sent overseas while not creating the excessive cost burden of an opt-in mechanism. It is important to note that all of these provisions should be structured as minimum protections that can be superseded, as need requires, by more traditional sectoral legislation.

The primary benefit of such generalized legislation would be a coherent data privacy framework for overseas BPO relationships. Such

a framework would ensure a minimum set of protections across sectoral lines and eliminate the loopholes that currently exist in the traditional patchwork of sectoral legislation. Further, such a framework would serve to clarify U.S. privacy expectations to Indian businesses. Finally, broad legislation of this sort would still remain cost-benefit justified because it would remain narrow enough, aimed only at a particular type of BPO relationship, to avoid traditional cost criticisms of exceedingly broad privacy legislation.

Finally, generalized overseas BPO legislation should be introduced because privacy is more than a mere economic commodity and demands more protections than the current utilitarian balancing affords. Allowing business concerns over cost to dominate discussion of privacy in the U.S.-Indian BPO relationship skews analysis in favor of business who can more easily quantify a numerical value for its position. This ignores important personal value placed on one's own privacy and leads to a regime of under-protection. Therefore, in order to protect privacy in the U.S.-Indian BPO relationship, legislation should establish a minimum level of protection to ensure that privacy is not commodified as an economic good and, therefore, is not under-protected as such a good.